

# THE CENTER FOR INTERNET SECURITY<sup>SM</sup>

## Deploying and Verifying Checklists The Keys to Widespread Adoption

Clint Kreitner  
[www.cisecurity.org](http://www.cisecurity.org)  
[ckreitner@cisecurity.org](mailto:ckreitner@cisecurity.org)

Better user understanding of what is causing  
the vulnerabilities that are being exploited

- Software defects
  - Fixed with vendor patches
- Lack of technical security controls
  - Security settings made to enable or disable security features of the OS software

Better user understanding of how high level standards tie with technical security settings

- ISO 17799
- COBIT from ISACA
- SysTrust, WebTrust from AICPA
- FISCAM from GAO
- Principles and Practices for Security of IT Systems from NIST
- Standard of Good Practice from ISF

3

The high level standards are helpful, but incomplete

- They describe “what” to do, but not “how”
- These standards are effective only when accompanied by details on how to implement their requirements

4

## *An Example from ISO 17799*

### *9.7.1 Event logging*

Audit logs recording exceptions and other security-relevant events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Audit logs should also include:

- a) user IDs
- b) dates and times for log on and log-off
- c) terminal identity or location if possible
- d) records of successful and rejected system access attempts;
- e) records of successful and rejected data and other resource access attempts.

5

One of several actions needed to implement event logging on Sun Solaris systems:

```
cat << END_SCRIPT >> /etc/inet.d/newperf
#!/sbin/sh
/usr/sbin/su sys -c \
"/usr/lib/sa/sa0 -f /var/adm/sa/sa0 date + '%d %T'"
END_SCRIPT
chmod 700 /etc/inet.d/newperf
chmod 744 /etc/inet.d/newperf
rm -f /etc/rc2.d/S21perf
ln -s /etc/inet.d/newperf /etc/rc2.d/S21perf
/usr/sbin/su sys -c cat << END_ENTRIES
0 20 40 * * * * /usr/lib/sa/sa1
45 20 * * * /usr/lib/sa/sa2 -s 0 00 -e 23 59 -f 1200 -f
END_ENTRIES
```

5

## Why has it been so difficult to proliferate good security practice?

- Vendors have been shipping systems to users with technical security controls turned off
- Users don't know how to properly configure their systems
- Users are afraid to disrupt operations
  - With patching or security settings

## Why else would this be true?

Microsoft Issues Patches, But Users Don't Apply Them		
	Attack date	Advance notice
SQL Slammer	1/25/03	185 days
Bugbear	9/30/02	502 days
Frethem	7/17/02	427 days
Yaha	6/22/02	402 days
ElKern	4/17/02	336 days
Klez	4/17/02	336 days
Badtrans	11/24/01	192 days
Nimda	9/18/01	336 days
Code Red	7/19/01	31 days
Average: 305 days		
Source: McAfee, MessageLabs, Microsoft, Symantec, and Sophos		

Forrester  
Research  
Report

April 3, 2003

## More sharply targeted configuration recommendations

- Different security levels
- Different system roles

## Different levels of hardening

- Levels of Security
  - Legacy – Level I
  - Enterprise – Level II
  - High – Level III (Gold Standard)

## Different system roles

- Role-based security benchmarks
  - Domain member workstation
  - Domain member server
  - Domain Controller
  - Standalone workstation
  - Standalone server
  - Laptop
  - Bastion Server
  - IIS Server
  - File & Print Server

11

## Benchmarks are needed for:

- Common OS/application combinations
  - Definitive verification of breakage via testing
- Appliances
  - Copiers, scanners, printers, etc.

12

## The importance of broad consensus among security experts

- There is such a thing as too many sources of guidance
  - How are users to choose from among those available?

13

## The crucial role of scoring tools

- Motivate behavior toward more robust security
- Enable tracking of configuration status over time
- Helps communication between security specialists and management

14

## How about:

- Databases of scores by sector
  - Anyone here want to be on the left hand side of the distribution curve?
  - The CI model works well here

15

**Windows NT/2000 Security Scoring Tool v2.1.2**

File Scoring Reporting Benchmarks Help

**THE CENTER FOR INTERNET SECURITY<sup>SM</sup>**

Computer: CLINT-NFV6O5590 **OVERALL SCORE: 8.5**

Scan Time: 08/19/2002 22:10:46

**Scoring**

**SCORE**

Select Security Template: Win2kProGold\_R1.2.inf

☒ Force Gold Standard Scoring (Win2K Professional ONLY)

**HFNetChk Options**

☐ Use Local HFNetChk Database.

mssecure.xml

☐ Do not evaluate file checksum.

☐ Do not perform registry checks.

☐ Verbose output.

**Compliance Verification**

INF File Comparison Utility

**Group Policy - Domain Users Only**

Export Effective Group Policy

**Reporting**

Summary Report Hotfix Report User Report Service Report Scan Log Debug Log

**Service Packs and Hotfixes**

Service Pack Level: 3 Score: 1.25

Hotfixes Missing: 0 Score: 1.25

**Account and Audit Policies**

Passwords over 90 Days: 2 Score: 0

Policy Mismatches: 0 Score: 0.8333

Event Log Mismatches: 0 Score: 0.8333

**Security Settings**

Restrict Anonymous: 2 Score: 1.25

Security Options Mismatches: 0 Score: 1.25

**Additional Security Protection**

Available Services Mismatches: 0 Score: 0.625

User Rights Mismatches: 0 Score: 0.625

NoLMHash: NTFS: 0 Score: 0.625

Registry and File Permissions: 12 Score: 0

Designed by Kerry Steele, Corey Badeaux, Paul Bible and Ron King.  
Please direct all feedback to: [Win2k-Feedback@cisecurity.org](mailto:Win2k-Feedback@cisecurity.org)



## The value of case studies

- (1) Scan a system “out of the box” and list identified vulnerabilities
- (2) Configure the system with the appropriate benchmark
- (3) Rescan the system and note the vulnerabilities remaining

17

## Vulnerability Assessment Case studies

<u>Study</u>	<u>System</u>	<u>Benchmark</u>	<u>% of Vuls Eliminated</u>
Solutionary	W2K Server	Level I	85
Citadel	W2K Pro	Level I	81
NSA	W2K Pro	Level II	91
Mitre	W2K Pro	Level II	83 (CVE)
Citadel	W2K Server	Level II	99
Citadel	RedHatLinux	Level I	100

## Encouraging progress

- Federal gov't promulgation of CIS benchmarks and tools via FedCIRC
- VISA adoption of CIS benchmarks for its Cardholder Information Security Program's Digital Dozen
- Progress at the vendor level
  - Dell's decision to offer pre-configured W2K systems
  - Top security experts from Microsoft, Sun, HP, Cisco, and Oracle are active on the benchmark teams
  - AOL's decision to work with CIS on an AOL User's benchmark and easy to use implementation tools

12

## Management benefits of using benchmarks and tools

- Substantially reduce the risk of unauthorized intrusion
- Following a recognized patching and configuration standard demonstrates due care against legal liability
- Provides a basis for ongoing measurement and reporting of security status to management
  - FISMA

20

## What will foster better configuration and patching practices?

- Incorporation in procurement req'ts by government and corporate buyers
  - Vendors will ship safer systems
- Compliance required by corporate audits
- Agencies serious about compliance with FISMA req'ts
- Organizational desire to demonstrate due care against potential legal liability

21

## What will foster better configuration and patching practices?

- Insurance premium discounts for demonstrated compliance
- ISP's getting in the game to make compliance with the "Big Four" easy for their customers
  - Anti-virus
  - Firewall
  - Up to date patching
  - Sound configuration practice

22

Thank you!

[chrlther@disecurity.org](mailto:chrlther@disecurity.org)  
<http://www.disecurity.org>

23